Vijeće
Europske unije

Bruxelles, 17. listopada 2022.
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	17. listopada 2022.
Za:	Delegacije
Br. preth. dok.:	12930/22
Predmet:	Zaključci Vijeća o sigurnosti lanca opskrbe IKT-a – zaključci Vijeća koje je Vijeće odobrilo na sastanku 17. listopada 2022.

Za delegacije se u Prilogu nalaze Zaključci Vijeća o sigurnosti lanca opskrbe IKT-a kako ih je Vijeće odobrilo na sastanku održanom 17. listopada 2022.

PRILOG

Zaključci Vijeća o sigurnosti lanca opskrbe IKT-a

VIJEĆE EUROPSKE UNIJE,

PODSJEĆAJUĆI na svoje zaključke:

– od 20. studenoga 2017. o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a”,

– o izgradnji kapaciteta i sposobnosti u području kibersigurnosti u EU-u,

– o važnosti mreža 5G za europsko gospodarstvo i potrebi za ublažavanjem sigurnosnih rizika povezanih s mrežama 5G,

– o oblikovanju digitalne budućnosti Europe,

– naslovljene „Oporavak kojim se pospješuje prijelaz prema dinamičnijoj, otpornijoj i konkurentnijoj europskoj industriji”,

– o kibersigurnosti povezanih uređaja,

– o Strategiji EU-a za kibersigurnost za digitalno desetljeće,

– o razvoju položaja Europske unije u pogledu kiberprostora,

– o tematskom izvješću Europskog revizorskog suda br. 03/2002 naslovljenom „Uvođenje 5G mreža u EU-u: bilježe se kašnjenja u uvođenju mreža, a određena sigurnosna pitanja i dalje nisu riješena”;

PODSJEĆAJUĆI na zaključke Europskog vijeća o:

– bolesti COVID-19, jedinstvenom tržištu, industrijskoj politici, digitalizaciji i vanjskim odnosima od 1. i 2. listopada 2020.,

– ruskoj vojnoj agresiji na Ukrajinu, sigurnosti i obrani, energetici, gospodarskim pitanjima, bolesti COVID-19 i vanjskim odnosima od 24. i 25. ožujka 2022.,

– Ukrajini, sigurnosti opskrbe hranom, sigurnosti i obrani te energiji od 30. i 31. svibnja 2021.;

1. s obzirom na sve veću važnost geopolitike za kibersigurnost ISTIČE da Europska unija i njezine države članice trebaju sveobuhvatno i strateški pristupiti kibersigurnosti. Zbog vojne agresije Rusije na Ukrajinu došlo je do velike promjene u strateškom i sigurnosnom okružju Europske unije te se pokazala potreba za snažnijom i sposobnijom Europskom unijom u području sigurnosti i obrane. Time je istaknuto da je iznimno važno na odgovarajući način uzeti u obzir geopolitičko okružje ne samo pri odgovoru na zlonamjerne kiberaktivnosti, već i pri izgradnji i održavanju otpornosti informacijskih i komunikacijskih tehnologija (IKT). To je posebno relevantno za lance opskrbe IKT proizvodima i uslugama (lanci opskrbe IKT-a), koji bi mogli biti ugroženi na temelju geopolitičkog suparništva, kao što je vidljivo iz napada na poduzeće SolarWinds, i na koje bi mogle utjecati geopolitičke napetosti i nestabilnost, što je vidljivo iz prijetnje povezane s ovisnošću o ruskim dobavljačima IKT-a u vrijeme ruske vojne agresije na Ukrajinu;

2. NAPOMINJE da priroda rizika povezanih s lancem opskrbe IKT-a, koji se sastoji od povezanog skupa resursa i procesa među gospodarskim subjektima (kako su definirani u Uredbi (EU) 2019/1020) koji počinje nabavom sirovina i obuhvaća proizvodnju, obradu i isporuku IKT proizvoda i usluga te rukovanje s njima, uključujući pružanje potpore tijekom životnog ciklusa IKT proizvoda i usluga, donosi jedinstvene izazove i potencijalno dalekosežne posljedice. Osim rizika povezanih s nedostupnošću IKT proizvoda, primjerice zbog nestašice kritičnih sirovina i poluvodiča potrebnih za njihovu proizvodnju, lanci opskrbe IKT proizvodima i uslugama izloženi su drugim prijetnjama. Konkretno, zlonamjerni akteri mogu ih ciljati ili zloupotrijebiti na sofisticirane, često prikrivene načine koji utječu na povjerljivost, cjelovitost i dostupnost prenesenih i pohranjenih osjetljivih podataka;

3. uviđajući da je potreban pristup kojim se obuhvaćaju sve opasnosti kako bi se osigurala IKT imovina, PREPOZNAJE važnost Prijedloga direktive o otpornosti kritičnih subjekata za poboljšanje fizičke sigurnosti kritičnih subjekata te ISTIČE da je, uz jačanje otpornosti na napade u lancu opskrbe koji se provode kibersredstvima, jednako važno ojačati opću otpornost i sigurnost lanaca opskrbe IKT-a u odnosu na cijeli niz čimbenika prijetnji, kao što su prirodne pojave, kvarovi sustava, unutarnje prijetnje ili ljudske pogreške. U tom smislu PREPOZNAJE da sigurnost lanca opskrbe IKT-a obuhvaća osiguravanje zaštite IKT proizvoda i usluga koji se proizvode, isporučuju, nabavljaju i upotrebljavaju u lancima opskrbe IKT-a, među ostalim zaštitom pojedinačnih komponenti i prenesenih podataka;

4. oslanjajući se na pouke izvučene iz posljedica strateških ovisnosti Europske unije o ruskim fosilnim gorivima, kao i iz učinaka poremećaja u lancima opskrbe tijekom pandemije bolesti COVID-19, osobito u pogledu farmaceutskih proizvoda i poluvodiča, pri čemu su bile izložene strateške ovisnosti EU-a, POTIČE države članice da rade na izbjegavanju sličnih situacija neželjenih strateških vanjskih ovisnosti u vezi s IKT proizvodima i uslugama. Zbog sve veće digitalizacije društva i sve veće upotrebe IKT-a u kritičnoj infrastrukturi, strateške vanjske ovisnosti povezane s IKT proizvodima i uslugama i njihovim lancima opskrbe trebalo bi stalno procjenjivati i, prema potrebi, rješavati;

5. PODSJEĆA da je postizanje strateške autonomije uz istodobno očuvanje otvorenog gospodarstva ključni cilj Unije, koji uključuje utvrđivanje i smanjenje strateških ovisnosti i povećanje otpornosti u najosjetljivijim industrijskim ekosustavima i specifičnim područjima, među ostalim u digitalnom području. To obuhvaća razvoj i uvođenje strateških digitalnih kapaciteta i infrastrukture te jačanje sposobnosti donošenja autonomnih tehnoloških odabira i, kao jedan od glavnih stupova, osiguravanje otpornih i sigurnih infrastruktura, proizvoda i usluga za izgradnju povjerenja u jedinstveno digitalno tržište i unutar europskog društva, pri čemu se održavaju otvorenost, globalna suradnja s partnerima sličnih stavova i konkurentnost i iskorištavaju potencijalne prednosti toga. Temeljne vrijednosti Europske unije osobito služe očuvanju privatnosti, sigurnosti, jednakosti, ljudskog dostojanstva, vladavine prava i otvorenog interneta kao preduvjetâ za ostvarenje društva, gospodarstva i industrije koji se temelje na digitalizaciji, a usmjereni su na čovjeka;

6. NAPOMINJE da je zbog razvoja kiberprijetnji vidljivog iz trenda izrazito učinkovitih i sofisticiranih napada u lancu opskrbe posljednjih godina, kao što su napadi na poduzeća SolarWinds, Mimecast ili Kaseya, koji se pojavljuju zajedno s eksternalizacijom osnovnih IKT usluga i pojačani su zbog ukupne ovisnosti o IKT proizvodima i uslugama koje proizvode, pružaju ili servisiraju treće strane, u budućnosti vrlo vjerojatno da će doći do većeg broja napada u lancu opskrbe sa znatnom štetom za gospodarstvo i društvo. S obzirom na to, ISTIČE važnost jačanja sigurnosti i otpornosti lanaca opskrbe IKT-a za funkcioniranje jedinstvenog tržišta, zajedno s potrebom da se osiguraju dostupnost, sigurnost i raznolikost IKT proizvoda i usluga na jedinstvenom tržištu. Stoga POZDRAVLJA potrebu za maksimalnim povećanjem i racionalizacijom upotrebe postojećih instrumenata i pristupa EU-a za ostvarenje tih ciljeva, kao i potrebu za kontinuiranom prilagodbom promjenjivim kiberprijetnjama uvođenjem dodatnih odgovarajućih mjera i mehanizama, među ostalim u vezi s mogućim sigurnosnim rizicima novih i disruptivnih tehnologija. POTIČE države članice da u tom pogledu nastoje primjenjivati pristup utemeljen na riziku kako bi se suočile s razvojem novih tehnologija;

7. PREPOZNAJE da je razumijevanje kiberprijetnji koje se stalno mijenjaju, kao i složenosti napada u lancu opskrbe, ključno za učinkovito ublažavanje rizika povezanih s lancima opskrbe IKT-a. U tom pogledu NAGLAŠAVA potrebu za prilagodbom novim prijetnjama putem aktivnog i kontinuiranog praćenja, analize i procjene prijetnji u lancu opskrbe, za podizanjem svijesti i izgradnjom znanja o prijetnjama i ranjivostima te za proaktivnim i prilagođenim upozoravanjem relevantnih subjekata. POZDRAVLJA rad Agencije Europske unije za kibersigurnost (ENISA) u vezi sa sigurnošću lanca opskrbe IKT-a, a posebice njezino izvješće o prijetnjama u vezi s napadima u lancu opskrbe;

MEĐUSEKTORSKI INSTRUMENTI I PRISTUPI

8. PONOVNO POTVRĐUJE važnost toga da države članice razmotre potrebu za diversifikacijom dobavljača ključnog IKT-a kako bi se izbjeglo ili ograničilo stvaranje velikih ovisnosti o jednom dobavljaču, a posebice o visokorizičnim dobavljačima, jer se time povećava izloženost posljedicama mogućih poremećaja. PREPOZNAJE izbjegavanje ovisnosti o određenom dobavljaču i diversifikaciju dobavljača IKT-a kao jednu od važnih sastavnica za osiguravanje stabilnosti i sigurnosti unutarnjeg tržišta. ISTIČE potrebu za promicanjem i provedbom odgovarajućih strategija kojima se na tehnološki neutralan način olakšava diversifikacija dobavljača i konkurentnost. Osim toga, POTIČE uključivanje aspekata povezanih sa sprečavanjem ovisnosti o određenom dobavljaču u zakonodavstvo EU-a. U tom pogledu POZDRAVLJA Prijedlog uredbe o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu (Akt o podacima), čiji je cilj povećati interoperabilnost usluga obrade podataka i ukloniti prepreke za promjenu pružatelja usluga obrade podataka;

9. PREPOZNAJE povezanost sigurnosti lanca opskrbe IKT-a s javnom nabavom. ISTIČE potrebu da se u postupcima javne nabave na odgovarajući način uzme u obzir važnost sigurnosti lanca opskrbe IKT-a uvođenjem, prema potrebi, objektivnih kriterija za odabir utemeljenih na riziku koji se odnose na sposobnost ponuditelja da osiguraju visoku razinu sigurnosti pruženih usluga. POZIVA na pronalaženje prave ravnoteže između javnog interesa za najučinkovitiju i najpravedniju upotrebu javnih sredstava s jedne strane i javnog interesa za osiguravanje informacijskih sustava i osiguravanje neometanog funkcioniranja jedinstvenog tržišta s druge strane. S ciljem olakšavanja provedbe relevantnih pravila o javnoj nabavi s obzirom na povećanje kibersigurnosti POZIVA Komisiju da do trećeg tromjesečja 2023. izradi metodološke smjernice kako bi se javne naručitelje potaknulo da se na odgovarajući način usredotoče na kibersigurnosne prakse ponuditelja i njihovih podugovaratelja te da procijeni relevantno zakonodavstvo o javnoj nabavi i, prema potrebi, da prijedloge za reviziju ili dopunu tog zakonodavstva;

10. PREPOZNAJE da bi izravna strana ulaganja povezana s IKT proizvodima i uslugama, iako pružaju gospodarske i socijalne koristi državama članicama, poduzećima i građanima, istodobno mogla uključivati rizike za sigurnost i javni poredak te NAPOMINJE da bi se mehanizam EU-a za provjeru izravnih stranih ulaganja, zajedno s odgovarajućim nacionalnim sustavima za provjeru, kojima se osiguravaju sredstva za rješavanje takvih rizika, mogao primijeniti i kao koristan alat za zaštitu sigurnosti i otpornosti lanca opskrbe IKT-a doprinosom uklanjanju visokorizičnih ulaganja koja mogu utjecati na takvu sigurnost i otpornost. UVIĐA da informacije koje se razmjenjuju i dijele putem tog mehanizma mogu pomoći državama članicama da bolje procijene moguće prijetnje sigurnosti lanaca opskrbe IKT-a i poduzmu potrebne korake u skladu s time. POZIVA relevantne nacionalne aktere da, prema potrebi, uzmu u obzir i tu dimenziju mehanizma za provjeru;

11. kad je riječ o obrani, PONOVNO POTVRĐUJE svoj poziv Komisiji da 2023., zajedno s državama članicama, procijeni rizike za lance opskrbe za kritičnu infrastrukturu u različitim područjima, uključujući digitalno područje, povezane sa sigurnosnim i obrambenim interesima EU-a te da istraži mogućnosti za povećanje kibersigurnosti u cijelom lancu opskrbe EU-ove obrambene tehnološke i industrijske baze. Nadalje, POZIVA države članice i Komisiju da razmotre sigurnost lanca opskrbe IKT-a u provedbi obveza i mjera iz Strateškog kompasa;

12. prepoznajući važnost kritičnih sirovina i svih vrsta poluvodiča kao osnovnih komponenti IKT proizvoda, POTIČE konstruktivne pregovore o Prijedlogu uredbe o uspostavi okvira mjera za jačanje europskog ekosustava poluvodiča (Akt o čipovima) i Prijedlogu uredbe Vijeća o izmjeni Uredbe (EU) 2021/2085 o osnivanju zajedničkih poduzeća u okviru programa Obzor Europa u pogledu Zajedničkog poduzeća za čipove;

INSTRUMENTI SPECIFIČNI ZA KIBERPODRUČJE

13. PREPOZNAJE, posebno u pogledu telekomunikacijske infrastrukture, postignuća na razini Unije za poboljšanje sigurnosti lanca opskrbe 5G mreža, posebno putem paketa instrumenata EU-a za sigurnost 5G tehnologije (paket instrumenata EU-a za 5G). POZIVA države članice da nastave razmjenjivati informacije o najboljim praksama i metodologijama u vezi s provedbom mjera preporučenih u okviru paketa instrumenata EU-a za 5G i posebno da za ključnu imovinu koja je u koordiniranoj procjeni rizika EU-a definirana kao kritična i osjetljiva primijene relevantna ograničenja na visokorizične dobavljače. ISTIČE da paket instrumenata EU-a za 5G predstavlja fleksibilan alat utemeljen na riziku za rješavanje utvrđenih sigurnosnih izazova, kojim se omogućuje pravodobno i učinkovito upravljanje kibersigurnosnim aspektima 5G tehnologije, uz istodobno poštovanje nadležnosti država članica te PREPOZNAJE da je taj paket vrijedan alat za daljnje koordinirano poboljšanje sigurnosti lanca opskrbe telekomunikacijskih mreža, uz potpunu transparentnost, koji bi mogao poslužiti kao nadahnuće za alate za procjenu i ublažavanje rizika povezane s drugim ključnim sektorima. PODSJEĆA na poziv relevantnim tijelima da na temelju procjena rizika izrade preporuke državama članicama i Komisiji kako bi se ojačale komunikacijske mreže i infrastrukture za otpornost u Europskoj uniji, uključujući nastavak provedbe paketa instrumenata EU-a za 5G;

14. PRIMA NA ZNANJE važnost interoperabilnih pristupa kojima se može riješiti pitanje ovisnosti o određenom dobavljaču i smanjiti koncentracijski rizik, uz istodobno poboljšanje sigurnosti lanca opskrbe u cijelom spektru infrastrukture i usluga IKT-a. PREPOZNAJE, posebno u odnosu na 5G mreže, potencijalne koristi koncepta otvorenog RAN-a u tom pogledu i istodobno PODSJEĆA na Izvješće o kibersigurnosti otvorenog RAN-a koje je objavila Skupina za suradnju NIS i u kojem se navodi da je taj koncept još u fazi razvoja i da su njegova sigurnost, transparentnost i standardizacija u ranoj fazi zrelosti te ISTIČE važnost procjene rizika prije svakog prijelaza na nove standarde ili strukture;

15. ISTIČE važnost postojećih i predstojećih horizontalnih zakonodavnih instrumenata u području kibersigurnosti za povećanje sigurnosti lanca opskrbe IKT-a, posebno Uredbe o ENISA-i (Agencija Europske unije za kibersigurnost) i Uredbe o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (Akt o kibersigurnosti), predstojeće Direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS 2), Prijedloga uredbe o utvrđivanju mjera za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije te Prijedloga uredbe o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima (Akt o kiberotpornosti). Osim toga, PRIMA NA ZNANJE važne promjene u sektorskim propisima o kibersigurnosti, posebno u budućoj Uredbi o digitalnoj operativnoj otpornosti za financijski sektor (DORA), koja uključuje nadzorni okvir za treće strane pružatelje IKT usluga koje su ključne za financijske subjekte. Tim se propisima uvode opće obveze povezane sa sigurnošću lanca opskrbe te detaljni i posebni zahtjevi relevantni za dotični sektor. Istodobno NAGLAŠAVA da dobavljači često isporučuju svoje proizvode i usluge različitim sektorima, a ne samo jednoj industriji. Stoga je iznimno važno osigurati da su zahtjevi u pogledu sigurnosti lanca opskrbe, u mjeri u kojoj je to moguće, usklađeni u svim relevantnim sektorima, posebno onima obuhvaćenima budućom Direktivom NIS 2, kako bi se izbjegle razlike među obvezama nametnutima dobavljačima te kako bi se subjektima u ključnim sektorima smanjilo opterećenje procjene usklađenosti dobavljača s tim obvezama, uzimajući pritom u obzir posebnosti sektora;

16. POZDRAVLJA Prijedlog akta o kiberotpornosti kao važan zakonodavni instrument za unapređenje sigurnog razvoja proizvodâ s digitalnim elementima i za osiguravanje toga da se kibersigurnost uzima u obzir u cijelom životnom ciklusu proizvodâ s digitalnim elementima. NAPOMINJE da Prijedlog akta o kiberotpornosti može znatno doprinijeti jačanju sigurnosti lanca opskrbe IKT-a. POTIČE konstruktivne pregovore i pravodobno donošenje Akta;

17. PREPOZAJE u tom pogledu rad koji ENISA trenutačno obavlja zajedno s državama članicama i drugim dionicima kako bi se EU-u pružili programi certifikacije za IKT proizvode, usluge i procese u skladu s Aktom o kibersigurnosti kojima bi se trebalo doprinijeti povećanju opće razine kibersigurnosti na digitalnom jedinstvenom tržištu. POTIČE sve dionike da sudjeluju u pripremnom radu na pojedinačnim europskim programima certifikacije kako bi se izgradilo povjerenje u sigurne IKT proizvode, procese i usluge i kako bi se ojačala njihova otpornost te POZIVA Komisiju da brzo izradi provedbene akte o europskim programima certifikacije nakon završetka pripremnog rada, posebno o europskom programu kibersigurnosne certifikacije (EUCC) koji se temelji na zajedničkim kriterijima. NAPOMINJE da bi europski programi certifikacije trebali uključivati, prema potrebi, zahtjeve u pogledu sigurnosti lanca opskrbe, uključujući odnose s dobavljačima;

18. ISTIČE potrebu za temeljitom provedbom svih odredaba predstojeće Direktive NIS 2 koje se odnose na sigurnost lanca opskrbe IKT-a. U tom pogledu NAGLAŠAVA važnost koordiniranih procjena rizika ključnih lanaca opskrbe na razini EU-a (koordinirane procjene rizika u lancu opskrbe), nacionalnih politika u području sigurnosti lanca opskrbe i sigurnosnih mjera povezanih s lancem opskrbe. NAPOMINJE da u pogledu rizika za sigurnost primarnog dobavljača ili krajnjeg klijenta ne bi trebalo posvetiti pozornost samo primarnim dobavljačima nego i relevantnim podugovarateljima. Kako bi se olakšala provedba mjera upravljanja rizicima u lancu opskrbe, POTIČE ENISA-u da uz pomoć Skupine za suradnju NIS provede pregled najboljih praksi dostupnih za upravljanje rizicima u lancu opskrbe i da ih objedini u metodološke smjernice. Osim toga, POTIČE ENISA-u da prati ulaganja u sigurnost lanca opskrbe IKT-a subjekata uređenih na temelju predstojeće Direktive NIS 2;

19. ISTIČE ujedno koristi i rizike od upotrebe pružatelja upravljanih usluga (MSP-ovi) i pružatelja upravljanih sigurnosnih usluga (MSSP-ovi) u kontekstu sigurnosti lanca opskrbe. Iako se upotrebom tih pružatelja usluga može znatno poboljšati sigurnost unutar organizacija i dovesti do viših razina kibersigurnosti, upravljanje IKT sustavima i uslugama na daljinu u kombinaciji s povlaštenim pristupom IKT okruženju klijenata, koje bi moglo biti potrebno MSP-ovima i MSSP-ovima, može u slučaju kompromitiranih MSP-ova ili MSSP-ova dovesti do negativnih kaskadnih učinaka na velik broj klijenata. Stoga je iznimno važno da MSP-ovi i MSSP-ovi održavaju visoku razinu vlastite unutarnje sigurnosti i sigurnosti usluga koje pružaju te da imaju transparentan pristup prema svojim klijentima u pogledu sigurnosti usluga koje pružaju. U tom pogledu POZDRAVLJA njihovo buduće uključivanje u područje primjene predstojeće Direktive NIS 2;

20. u pogledu provedbe mehanizma za koordinirane procjene rizika u lancu opskrbe na temelju predstojeće Direktive NIS 2 PRIMA NA ZNANJE važnost netehničkih čimbenika rizika u tom kontekstu, kao što je neprimjeren utjecaj treće zemlje na dobavljače i pružatelje usluga, te u tom kontekstu PREPOZNAJE čimbenike koji se mogu upotrijebiti za procjenu profila rizika kako je navedeno u koordiniranoj procjeni rizika kibersigurnosti 5G mreža na razini EU-a. POZIVA Komisiju da do drugog tromjesečja 2023., nakon savjetovanja sa Skupinom za suradnju NIS i ENISA-om, da prednost utvrđivanju posebnih IKT usluga, sustava ili proizvoda koji bi mogli podlijegati koordiniranim procjenama rizika u lancu opskrbe;

21. NAPOMINJE da ovisnosti o visokorizičnim dobavljačima IKT proizvoda i usluga koji se upotrebljavaju za rad ključnih mreža i sustava predstavljaju stratešku prijetnju koju treba ublažiti odgovarajućim politikama na nacionalnoj razini i razini EU-a te suradnjom među državama članicama i s međunarodnim partnerima sličnih stavova. Kako bi se olakšalo ublažavanje tog strateškog rizika i poduprle koordinirane procjene rizika u lancu opskrbe, POZIVA Skupinu za suradnju NIS da u suradnji s Komisijom i ENISA-om razvije paket mjera za smanjenje ključnih rizika u lancu opskrbe IKT-a (paket instrumenata za lanac opskrbe IKT-a). Paket instrumenata za lanac opskrbe IKT-a trebao bi se temeljiti na strateškim scenarijima prijetnji utvrđenim za lance opskrbe IKT-a i sadržavati mjere za odgovor na te scenarije na temelju iskustava iz paketa instrumenata za 5G i onih stečenih na nacionalnoj razini. Njime bi se na transparentan način trebale dopuniti koordinirane procjene rizika u lancu opskrbe za posebne IKT usluge, sustave ili proizvode u okviru predstojeće Direktive NIS 2 ponudom općih mjera za smanjenje rizika koji se mogu prilagoditi posebnim IKT uslugama, sustavima ili proizvodima na prilagodljiv način, na temelju rizika utvrđenih u pojedinačnim koordiniranim procjenama rizika u lancu opskrbe;

22. NAGLAŠAVA važnu ulogu koju istraživačke, inovacijske, investicijske i poduzetničke aktivnosti u digitalnom području i području kibersigurnosti te financiranje takvih aktivnosti imaju kad je riječ o izbjegavanju mogućih neželjenih strateških ovisnosti u budućnosti i jačanju opće otpornosti lanaca opskrbe IKT-a. U tom kontekstu ISTIČE ulogu i važnost strateških i provedbenih zadaća Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) i mreže nacionalnih koordinacijskih centara za doprinos maksimalnom povećanju učinaka ulaganja radi jačanja vodstva i otvorene strateške autonomije Unije u području kibersigurnosti, potpore tehnološkim kapacitetima i vještinama Unije te povećanja globalne konkurentnosti Unije. U tom pogledu POZIVA na brzu operacionalizaciju ECCC-a. POZIVA ECCC da u svom strateškom programu uzme u obzir sigurnosne aspekte lanca opskrbe IKT-a, uključujući, na primjer, siguran razvoj softvera, uz istodobno osiguravanje dosljednosti i komplementarnosti te izbjegavanje udvostručavanja napora. PODUPIRE poboljšanje europske konkurentnosti u području kibersigurnosti putem programa financiranja, kao što su program Obzor Europa za istraživanja i inovacije te program Digitalna Europa za jačanje, izgradnju i stjecanje ključnih kapaciteta za digitalno gospodarstvo, društvo i demokraciju EU-a;

MEHANIZMI POTPORE

23. POTIČE jačanje poticaja za financijsku potporu povezanih s mjerama usmjerenima na jačanje sigurnosti lanca opskrbe IKT-a. POZIVA ECCC, Komisiju i relevantne dionike da, među ostalim s obzirom na predstojeću provedbu Direktive NIS 2, prioritetno istraže mogućnosti za uključivanje sigurnosnih aspekata lanca opskrbe IKT-a u predstojeće pozive u okviru programa rada u području kibersigurnosti u sklopu programa Digitalna Europa i programa Obzor Europa ili bilo koje druge relevantne mogućnosti financiranja. Te bi mogućnosti financiranja trebale, među ostalim, biti usmjerene na to da se organizacijama omogući da podrže održavanje visoke razine kibersigurnosti u pogledu nabave IKT proizvoda i usluga u cijelom lancu opskrbe, posebno u odnosu na zamjenu posebnih ključnih IKT usluga, sustava ili proizvoda koji su priznati kao visokorizični u skladu s budućim koordiniranim procjenama rizika u lancu opskrbe.

24. PREPOZNAJE da globalizacija i specijalizacija IKT usluga te povećana ovisnost o proizvodima i uslugama trećih strana dovode do potrebe za bliskom suradnjom unutar EU-a i na međunarodnoj razini u razmjeni znanja i stručnosti među relevantnim dionicima te ih POTIČE da pronađu snažan i koordiniran položaj kojim se na sveobuhvatan način osigurava sigurnost lanca opskrbe IKT-a. PREPOZNAJE i potrebu za daljnjim istraživanjem relevantnih najnaprednijih pristupa i tehnika u pogledu odgovarajuće osnovne kiberhigijene i dugoročnih rješenja za postizanje sigurnih i otpornih lanaca opskrbe IKT-a, kao i najprikladnijih načina njihova promicanja i mogućeg uključivanja u politike ili druge inicijative. U tom pogledu UVIĐA da bi posebnu pozornost trebalo posvetiti istraživanju koristi i nedostataka sustavnih rješenja, kao što su načela nultog povjerenja, softverski popis materijala i slična dugoročna rješenja. PREPORUČUJE da se za tu svrhu zaduži Skupina za suradnju NIS;

25. PRIMA NA ZNANJE koristi praćenja i djelotvorne razmjene informacija o kiberincidentima i kiberprijetnjama za sprečavanje, otkrivanje i ublažavanje učinaka napada u lancu opskrbe. ISTIČE potrebu za nastavkom izgradnje povjerenja i pouzdanja među državama članicama radi djelotvorne razmjene takvih informacija. PODSJEĆA u tom pogledu na prijedlog Komisije da se državama članicama pruži potpora u uspostavi i jačanju centara za sigurnosne operacije (SOC-ovi) kako bi se diljem EU-a izgradila mreža centara za sigurnosne operacije radi daljnjeg praćenja i predviđanja signala napada na mreže. PODSJEĆA na potrebu za komplementarnošću i koordinacijom u okviru postojećih mreža i mehanizama te u tom pogledu posebno ISTIČE ulogu mreže CSIRT-ova i potrebu za daljnjim istraživanjem potencijala tih mreža kako bi se promicala učinkovita, sigurna i pouzdana kultura razmjene informacija. PODSJEĆA na napore koje su države članice, uz potporu EU-a, poduzele kako bi uspostavile sektorske, nacionalne i regionalne CSIRT-ove i nacionalne ili europske centre za razmjenu i analizu informacija (ISAC-i) kao dio djelotvorne mreže kibersigurnosnih partnerstava u Uniji.

26. Zbog međusobno povezane i globalne prirode prijetnji u lancu opskrbe IKT-a ISTIČE važnost pristupa i poboljšanja sigurnosti lanca opskrbe IKT-a na globalnoj razini. S obzirom na to, PREPORUČUJE upotrebu digitalnih partnerstava, kiberdijalogâ i drugih relevantnih inicijativa EU-a, uključujući, prema potrebi, sporazume o slobodnoj trgovini, za promicanje evaluacija koje se temelje na riziku dobavljača IKT proizvoda i pružatelja IKT usluga, upotrebu pouzdanih dobavljača i primjenu sigurnog i inovativnog digitalnog ekosustava koji se temelji na otvorenim, interoperabilnim i transparentnim standardima. Osim toga, PONOVNO POTVRĐUJE viziju partnerstava u okviru strategije Global Gateway, kao i Vijeća za trgovinu i tehnologiju EU-a i SAD-a te aktivnosti u okviru njegovih radnih skupina, da se promiče upotreba pouzdanih dobavljača / dobavljača koji nisu visokorizični i razvije mehanizam financiranja kojim se omogućuju projekti s pomoću kojih infrastruktura i usluge IKT-a u trećim zemljama postaju sigurnije, otpornije i pouzdanije, među ostalim suzdržavanjem od financiranja kupnje od nepouzdanih/visokorizičnih dobavljača na tehnološki neutralan način;

27. PONOVNO POTVRĐUJE svoju predanost doprinošenju otvorenom, slobodnom, globalnom, stabilnom i sigurnom kiberprostoru i promicanju kiberprostora te poštovanju normi, pravila i načela odgovornog ponašanja država u kiberprostoru utvrđenih u okviru UN-a. Posebno kad je riječ o sigurnosti lanca opskrbe IKT-a, PODSJEĆA na normu koju su podržale skupine vladinih stručnjaka UN-a (UN GGE) i otvorene radne skupine (OEWG) kojom se države potiču na poduzimanje razumnih koraka s ciljem osiguravanja integriteta lanca opskrbe, među ostalim razvojem objektivnih mjera suradnje, kako bi krajnji korisnici mogli imati povjerenje u sigurnost IKT proizvoda i kako bi se nastojalo spriječiti širenje zlonamjernih alata i tehnika IKT-a i upotreba štetnih skrivenih funkcija te SE ZALAŽE za njihovu široku provedbu.